



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,560	06/19/2003	Myungsun Kim	DE-1484	6060

1109 7590 11/13/2006

ANDERSON, KILL & OLICK, P.C.  
1251 AVENUE OF THE AMERICAS  
NEW YORK,, NY 10020-1182

EXAMINER
----------

NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 11/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/600,560

Applicant(s)

KIM ET AL.

Examiner

Andrew L. Nalven

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 11 August 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2,7 and 8 is/are rejected.
- 7) ☒ Claim(s) 3-6 and 9-12 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 June 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

1. Claims 1-12 are pending.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. **Claim 1 is rejected under 35 U.S.C. 102(e)** as being anticipated by Gentry et al US PGPub 2003/0182554.

3. **With regards to claims 1 and 7**, Gentry teaches generating system parameters  $G_1$ ,  $G_2$ ,  $P$  and  $e$  and storing the system parameters in memory by a system administrator wherein  $G_1$  and  $G_2$  are cycle groups of order  $m$ ,  $P$  is a generator on the cyclic group  $G_1$ ,  $e$  is bilinear map defined as  $e: G_1 \times G_1 \rightarrow G_2$  (Gentry, paragraphs 0021-0022), generating a private key  $\langle a, b, c \rangle$  and a public key  $v$  and storing the public key  $v$  in the memory of a prover or the system administrator wherein  $a$ ,  $b$ , and  $c$  are randomly chosen in  $Z_m$  where  $Z_m$  is a multiplicative group of order  $m$  (Gentry, paragraphs 0021-0022), generating random numbers  $r_1, r_2, r_3$  of the group  $Z_m$  for obtaining an evidence  $(x, Q)$  and sending the evidence to a verifier by the prover

(Gentry, paragraphs 0020-0022), receiving the evidence (x, Q), selecting a randomly w of the group  $Z_m$  to obtain a query R, storing the evidence and the randomly selected number w in the memory and sending the query R to the prover by the verifier (Gentry, paragraphs 0022-0025), receiving the query R, computing a temporary value S to obtain a response Y and sending the response Y to the verifier by the prover (Gentry, paragraphs 0022-0025), and determining a legitimacy of the prover by employing the system parameters G1, G2, P and e, the public key v, the evidence (x, Q), and the randomly selected number w by the verifier (Gentry, paragraph 0024).

4. **With regards to claims 2 and 8**, Gentry teaches the public key v obtained by  $v = e(P, P)^{abc}$  (Gentry, paragraph 0021).

#### ***Allowable Subject Matter***

5. **Claims 3-6 and 9-12 are objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

6. **With regards to claims 3 and 9**, the cited prior art fails to teach a first evidence value  $x = e(P, P)^{r_1 * r_2 * r_3}$  and a second evidence value  $Q = r_1 * r_2 * r_3 * P$ . As a result, the cited prior art fails to anticipate or render obvious the above-cited claims.

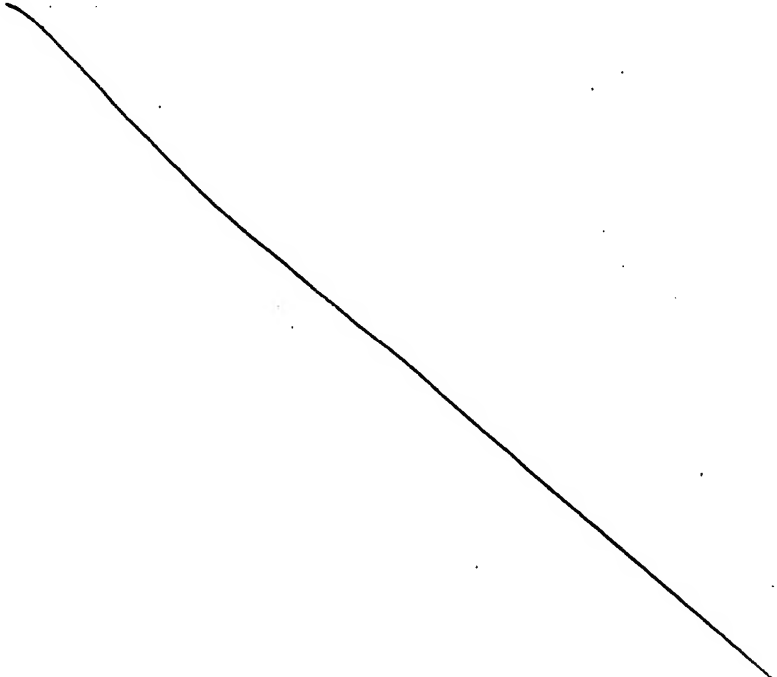
***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. Boneh et al US Patent No. 7,113,594 discloses a system for identity based encryption and related cryptographic techniques.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

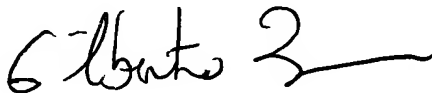
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571 272 3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven  


  
GILBERTO BARRÓN JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100